

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)	
)	
Protecting the Privacy of Customers of Broadband)	WC Docket No. 16-106
and Other Telecommunications Services)	

REPLY COMMENT SUPPLEMENT

It is deplorable that the Federal Bureau of Investigation and United States Secret Service (namely, General Counsel and Chief Counsel) filed joint reply to comments on July 5 without any reference to other comments or commenters. Their *comments* were due by May 27.

It is also deplorable that on April 29 the Commission ordered denial of “requests for an extension of time to file comments and reply comments in response to the *Broadband Privacy NPRM*, as filed by the Association of National Advertisers (ANA), the State Privacy & Security Coalition, Inc.”¹ (SPSC), et al., and yet without any reason except for “voluminous record” the reply comment deadline was extended five days before the deadline for an additional nine days. Who took advantage of that? ANA and SPSC.² And where is the petition for reconsideration?

Americans do not trust the Government, because rules and laws are so conspicuously and selectively discarded without accountability whatsoever. Why did the FBI and Secret Service file joint comments primarily regarding national security on the same day that the FBI Director made a public statement about extreme carelessness pertaining to national security? The FBI has sent mixed messages: one is that national security is threatened by “bad” actors via Internet access, and the other is that national security is threatened by official carelessness via Internet access.

The joint FBI and Secret Service filing directly linked national security with BIAS when any provider in America could not involve more than perhaps 7% of American consumers—less than credit card companies, banks and stores, such as Target. The Commission should ask: What exactly could be deemed a national security risk if an Internet customer’s personal information was compromised? Identity theft is *not* a national security matter, especially via smaller BIAS providers. But an alarming statement is found in their filing:³

“[t]he Federal Law Enforcement Agencies submit that a customer should receive notice if their customer proprietary information has been or is reasonably believed by the Service Provider to have been accessed or acquired by an unauthorized party, unless there is no reasonable risk of harm to the customer from the compromise of the information.”

¹ Para. 1 of Order, DA 16-473, WC Docket No. 16-106; adopted and released on April 29, 2016.

² Both filed on the second to last day of the extension: July 5.

³ Filed July 5, 2016.

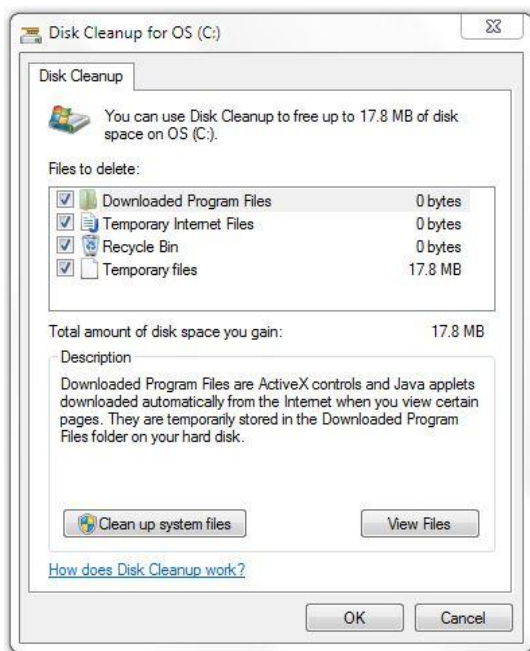
Pursuant to their suggestion, oversight and accountability could easily be circumvented for a data breach by arbitrarily deciding that no risk of harm existed. Can it not be plainly stated that private sector monitoring and surveillances, etc., occur without perceived harm, including utilizing linkable information?

Don't forget about me as rules and guidelines are established. My predicament continues, so let me share a personal experience of what occurred between 9-10 p.m. on July 4 as fireworks resounded throughout the city of Turlock.

I've described how I remain indigent and access the Internet with my Wi-Fi only third-generation iPad and six-year-old laptop primarily at a library four blocks away. However, I recently learned of free Wi-Fi at a nearby business. I'll minimize providing details by just stating that *many* planes have flown over after I've accessed the Internet at that location, as well.

For the first time, in the morning of July 4, I accessed the Internet outside the location with my laptop instead of my iPad. Noticeably not a single plane flew in the sky, which was the first time in eight months; and I thought that perhaps the surveillances had finally stopped. Later that evening I relaxed and left my laptop in sleep mode instead of unplugging it and removing the battery when unused. At 9:00 p.m. as I was stood outside and fireworks were popping around me I witnessed an operation against me.

A large white jet with lights that did not blink like a commercial airplane flew overhead. When it reached directly above me a helicopter flew very fast toward me then slowed above me and turned. A small plane suddenly appeared flying very low and fast. The helicopter repeated the same maneuver at least eight (8) times. The small plane whizzed by at least five (5) times, so low that I thought fireworks may hit it. Additionally, two other planes were crisscrossing above me. Finally I decided to go unplug my laptop, but I first ran Disk Cleanup and saw the following:



I am absolutely sure that not a single file was present for Disk Cleanup when my laptop was put in sleep mode earlier that evening. All of these personal experiences are expressed in context of the Commission's NPRM.

There is more than one reason why I personally would continue to be under surveillance, in which it is undeniable that when I access the Internet I often soon see a plane fly overhead no matter what time day or night. It is also undeniable that someone has used the Cisco device at the business to block me from going to certain websites, such as related to virtual private networks (VPNs), and I sporadically get a connection error when trying to use the privacy app, StartPage, on my iPad.

But there's another reason why I have likely been subjected to continued surveillance. On June 29, 2016 I formally alleged through the New York Attorney General's office that the vice president of a major collection agency made a false written statement, offering a false instrument for filing in the second degree—punishable as misdemeanors⁴—in connection to my account with Charter Communications. I then emailed two directors of Charter based in New York since my billing dispute has remained open and unresolved since April 2014.

We live in a world today in which a BIAS provider—or its able supporters—can send planes and helicopters to intercept cordless phone calls, Internet accesses, follow vehicles and infiltrate and electronically harm personal devices, while the FBI and Secret Service use isolated tragedies to gain access to myself and everyone else in the name of national and cyber securities.

Those agencies asked the Commission to control “the entity to notify the protectee.”⁵ If there is concern that special agency notifications are necessary, then that treatment should pertain only to public officials and national public figures. In no way do I need the FBI to notify me of a data breach, no matter what the situation or circumstance.

I learned long ago not to give in to fanaticisms of pending dangers from radicals. When I was in the Air Force during the buildup of the first American (coalition) war in Iraq, I was told repeatedly that Saddam Hussein had smuggled in chemicals and was going to release them at the military bases across the continental U.S. There was a big push for everyone at the military base in California to have a working gas mask, but it was all smoke and mirrors.

There is not the slightest likelihood of a person or group causing a national security risk involving common personal information via a BIAS provider. Truly, what could be utilized of customers that could cause national risk, and that customers could not be notified, and promptly? Personally, I guess a rogue actor could locate my devices like others do, and they could track my mom's and sister's cars via SiriusXM vehicle information like others do.

⁴ §175.30 and §210.45 of the Penal Law. As a side note, the vice president of the collection agency provided the New York Attorney General's Suffolk regional office a reply to my February 2016 complaint, but the regional office provided me a copy of that reply 97 days later, after the Charter/Time Warner merger was approved. [Ref., pg. 3 of my March 5, 2016 letter filed for MB Docket No. 15-149.]

⁵ From joint comments by FBI and Secret Service filed July 5, 2016 (at “1. LAW ENFORCEMENT SHOULD BE ABLE TO DELAY NOTIFICATION....”)

The involvement of federal law enforcement agencies in making decisions regarding data breach notifications should be clearly defined, to allow customers to make decisions themselves, likely minimizing loss, and to make sure that corporations are not allowed to hide behind third-party decisions. Bluntly, what the FBI and Secret Service's joint comments suggest could open a door for collusion between providers and agencies regarding delay or deference of notifications.

The ANA, on the other hand, wants the FCC to think an opt-in rule would create "notice fatigue,"⁶ but why would there be "a constant barrage of choice notifications"⁷ if the NPRM only relates to BIAS? The ANA implies BIAS providers would have their hands tied while customers would have to continually opt-in as they surfed the web.

The NPRM either encompasses edge provider services, burdens and consequences, or it doesn't. If the Commission omits incorporating edge providers within the ruling, then ideas of consequences and burdens caused by edge providers while accessing the Internet are irrelevant.

The other day I approached a career AT&T employee working on the telephone box near my residence asking what he was doing. He said, "Oh, you think I'm doing something to monitor your phone calls? ... This is what I tell anyone concerned about that: If you're not doing anything wrong, you don't have anything to worry about. If you're concerned, it generally means you're doing something wrong."

Please don't compromise public interests for corporate benefits. Please don't mishandle customers of BIAS as though they must enrich the provider. Please don't succumb to fanaticism concerning national security for residential customers of broadband service.



Shawn Sheridan
290 N. Thor St., Apt. 200
Turlock, CA 95380-4000
sheridan3398@yahoo.com

July 6, 2016

⁶ Pg. 1, reply comment of the Association of National Advertisers, filed July 5, 2016.

⁷ *Ibid.*, pg. 5.